DEVIANT BEHAVIOR
https://doi.org/10.1080/01639625.2018.1461786

Routledge
Taylor & Francis Group

Under the Corporate Radar: Examining Insider Business Cybercrime Victimization through an Application of Routine Activities Theory

Matthew L. Williams[a], Michael Levi[a], Pete Burnap[a], and R.V. Gundur[b]

[a]School of Social Sciences, Cardiff University, UK; [b]Department of Sociology, Social Policy & Criminology, Singapore

ABSTRACT

Cybercrime is recognized as one of the top threats to UK economic security. On a daily basis, the computer networks of businesses suffer security breaches. A less explored dimension of this problem is cybercrimes committed by insiders. This paper provides a criminological analysis of corporate insider victimization. It begins by presenting reviews of insider criminal threats and routine activities theory as applied to cybercrime. Analysis of the nationally representative Cardiff University UK Business Cybercrime Survey then informs statistical models that predict the likelihood of businesses suffering insider cyber victimization, using routine activities and guardianship measures as predictors.

ARTICLE HISTORY
Received 12 January 2018
Accepted 24 March 2018

Introduction

The imagery of cybercrime victimization is principally one of attacks by *outsiders*, whether "organized criminals" committing identity theft illegally transferring funds to themselves, or state-sponsored hackers committing economic and/or political espionage. The focus of this article, however, is on an understudied form of cybercrime victimization: *insider* business cybercrime. The risks from insiders have a long political history, and over the last century, concerns about "fifth columnists" and spies within the intelligence services and government have been a regular theme of counter-intelligence efforts. Though argument still exists about whether he was influenced by foreign powers, the mega-leak by Edward Snowden focused the attention of governments and corporations on insider cyber-security breaches. While such high-profile cases bring insider threats to the fore of political, law enforcement, and public attention, very little is known about the enabling and inhibiting situational factors of insider corporate cyber victimization. This paper is one of the first in criminology to apply Routine Activities Theory (RAT) to insider cybercrime within organizations via an analysis of the nationally representative Cardiff University UK Business Cybercrime Survey.

Cybercrime is officially viewed as one of the top threats (along with terrorism) to UK economic and national security (HM Government 2015).[1] To combat the growing and rapidly evolving cyber threat, the UK Government has invested circa £2 billion in cyber security between 2016 and 2021, including resources for businesses to guard themselves against victimization.[2] The Information Security Breaches Survey (ISBS) 1998–2015, the UK Government's flagship organizational cyber security survey, has routinely recorded relatively high levels of business cybercrime, including virus infection, hacking, fraud and insider cyber security breaches.

This latter type of business cybercrime victimization is understudied. The statistics that are available within the UK show that insider threats are on the increase (ISBS 2015). This increase has been

CONTACT Matthew L. Williams WilliamsM7@cf.ac.uk School of Social Sciences, Cardiff University, King Edward VII Ave, Cardiff, CF10 3WT

[1]Though it is not always clear where cybercrimes as national security threats end and cybercrimes as "human security" or ordinary threats begin. Data compromises may start as ordinary threats but end in national security ones, and vice versa. There is an element of subjectivity in play here.

[2]For example, Cyber-security Information Sharing Partnership (CiSP) and the National Cyber Security Center.

accounted for, in part, by the introduction of new technologies in the workplace, such as remote access, cloud computing, and social media, that alter *situational* and *environmental* contexts, presenting new opportunities for insider deviant activity. The insider cyber security threat can also subvert more typical business *guardianship* precautions, which have been based on the perception that cybercrime perpetrators are largely professional (or semi-professional) in criminal skills, are external in origin (often residing in another country) and are beyond the reach of local criminal justice agencies (Levi et al. 2016; Levi and Williams 2013; Maimon et al. 2014; Wall and Williams 2007, 2013; Williams 2006, 2007, 2016). When the focus of protection is on stopping outsider penetration, organizations can be left vulnerable to attacks originating from those seemingly "law-abiding" employees with inside knowledge of, and access to, systems, security processes, and trade secrets.

The impact of new technologies and inadequate security on the likelihood of insider victimization can be estimated using Routine Activities Theory (Cohen and Felson 1979). Several empirical applications point to the significant effect that frequent routine activity and the lack of capable guardians have on opening-up opportunities for cybercrime (Holt and Bossler 2008; Van Wilsem 2011; Williams 2016). This paper extends this work to explore whether corporate insider cybercrime victimization is a function of risky routine activities conducted in organizations that lack capable guardianship.

Definition and prevalence of insider business cybercrime

The work of Collins et al. (Collins et al. 2016:3) on insider victimization is perhaps the most extensive. Focused on the US, the authors develop a definition of malicious and unintentional insider threats based on an analysis of 734 cases known to the Computer Emergency Response Team (CERT) at Carnegie Mellon University:

Malicious Insider Threat: A current or former employee, contractor, or business partner who meets the following criteria:

- Has authorized access to an organization's network, system, or data and has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.

Unintentional Insider Threat: A current or former employee, contractor, or other business partner who:

- Has authorized access to an organization's network, system, or data and has no malicious intent associated with his or her action (or inaction) that caused harm or substantially increased the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems.

Collins et al. (2016:6) classified the cases studied into four classes of malicious insider cyber victimization (these cases did not include espionage or unintentional damage):

- 44 percent were classified as fraud—an insider's use of IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain, or theft of information that leads to an identity crime (e.g., identity theft or credit card fraud);
- 22 percent were classified as information technology (IT) sabotage—an insider's use of IT to direct specific harm at an organization or an individual;

- 21 percent were classified as theft of IP—an insider's use of IT to steal IP from the organization. This category includes industrial espionage involving outsiders;
- 17 percent were classified as miscellaneous—cases in which the insider's activity was not for IP theft, fraud, or IT sabotage.

It was found that the US banking and finance sectors suffered the greatest amount of insider victimization, followed by IT, healthcare, government, and commercial facilities.

In the UK, Levi and Gundur (2015) identified four types of corporate insider victimization in their analysis of circa 100 cases reported in the global media: (i) insider victimization without malicious intent; (ii) insider victimization with altruistic intent; (iii) insider victimization with malicious intent that may result in civil litigation; and (iv) insider victimization with malicious intent that may result in criminal litigation. Insider victimization without malicious intent is the result of an employee failing to follow best practices or by inadvertently engaging in an act that is detrimental to the economic interests of the company (e.g., using unsecured systems, employing weak passwords, etc.). Insider victimization with altruistic intent involves employees acting as "whistle-blowers." Arguably the most famous case involved the former NSA contractor Edward Snowden. Insider victimization with malicious intent that may result in civil litigation is typically due to an employee of a company moving to a competitor with confidential data or knowledge from his/her previous employer.

Insider victimization with malicious intent that may result in criminal prosecution can be divided into five prominent sub-classes: i) disruption or destruction; ii) embezzlement; iii) industrial espionage; iv) insider trading; and v) secure data theft (including but not restricted to identity theft). Each of these, if discovered and successfully prosecuted, typically result in a criminal conviction. Disruption and destruction is not common and is typically the work of disgruntled ex-employees who have technological expertise and attempt or conduct a cyberattack against their former employers, resulting in systems failures or the erasure of data or economic losses. Embezzlement is the largest sub-class of malicious insider crimes, disproportionately affecting financial institutions. Industrial espionage is perhaps the greatest insider threat to a company's wellbeing, given the potential for significant loss in terms of market share. Insider trading is a relatively common abuse of position where a person who is in position to take advantage of insider information does so and executes a scheme, typically over a substantial number of years, which allows them to enrich themselves. Secure data theft involves the abuse of privileged positions to steal personal data on customers and clients, which are used to create false accounts or sold on to others who are better placed to monetize the information. Often, acts of secure data theft are part of large criminal operations, which involve several outsiders gaining access to insiders and convincing them, either through coercion or reward, to steal confidential data. Identity theft is therefore the most common result in secure data theft.

Data on the prevalence of insider victimization in the UK are limited. The Home Office Commercial Victimization Survey (arguably the most authoritative survey on business related crimes in the UK) does include questions on cybercrime, but it does not distinguish insider victimization. The only other available Government source on business cybercrime is the ISBS, administered by the Department for Business, Energy and Industrial Strategy. This survey has included a question on insider victimization since 1998, and its 2015 sweep found high levels of prevalence in large corporations (75 percent recorded breaches), up 58 percent on the previous year (BIS 2015). However, the 2015 sweep did not use a random probability sampling strategy, meaning the results were not representative of the UK population of businesses.[3] The latest versions of this survey, the Cyber Security Breaches Survey 2016, did use a random probability sampling design, but it did not pose questions relating to insider cyber breaches. The data reported in this paper from the Cardiff University UK Business Cybercrime Survey therefore represent the most authoritative picture of the insider threat problem at the time of publication.

[3]Non random samples are likely to suffer from voluntary response bias, a form of sampling bias where respondents are self-selecting volunteers. Resulting samples are likely to be biased towards respondents with strong opinions, high levels of knowledge of the subject matter, and in the case in question, experience of victimization.

Insider cybercrime: a routine activities theory perspective

The criminological literature on insider victimization is sparse. Most of the literature under the rubric of "white-collar crime," for example, deals with the malefactions of corporate elites, in either corrupt or "revolving door" relationships with regulators, or involving rogue unit staff (acting for their staff and/or themselves). Gill's (2005) research did look at insider victimization, but only non-cyber fraud. Gill noted some victimization was enabled by the high levels of trust and autonomy given to potential offenders, that enabled actions to go unnoticed. Corrupt company/industry culture also correlated with victimization (see Discussion). It is reasonable to assume that these factors may be likewise present for insider cyber victimization. Routine Activities Theory provides potentially useful criminological insight into insider cyber victimization, which resonates with Gill's findings. For example, position of trust equates to routine activity and opportunity, and lack of visibility equates to absence of capable guardianship. It may therefore be fruitful to apply RAT to understand the likelihood of insider cyber victimization when only victim survey data are available; it should be stressed that opportunities are necessary but not sufficient conditions for insider and any other crimes. RAT posits that the likelihood of victimization increases when an attractive target and a lack of a capable guardian intersect with a motivated offender in time and space (Cohen and Felson 1979). It has been found to be particularly applicable to cybercrime as it is not reliant upon complex understandings of the motivations of offenders (Williams 2016). Cybercrime researchers are less likely to focus on offender motivations given low levels of apprehension by law enforcement. In one of the first evaluations of RAT as applied to cybercrime the following factors were found to be significant in predicting victimization: Visibility of target (heightened by the regularity and range of online routine activities) and accessibility of target (heightened by the lack of a capable guardian) (Newman and Clarke 2003).

There is currently no research that empirically applies RAT to business cybercrime. However, there are a number of studies based on the domestic population. Studies of cyber-harassment and computer virus infection have shown proximity to motivated offenders and varied and intense online routine activity were predictive of victimization (Holt and Bossler 2008; Van Wilsem 2011). Perhaps most pertinent to insider cyber victimization, studies of online identity theft among domestic victims have produced some encouraging results. Online routine activities, including Internet banking, shopping, emailing, and downloading, have consistently been found to statistically predict domestic online identity theft victimization in the US, the Netherlands, the UK, and Europe (Pratt, Holtfreter, and Reisig 2010; Reyns 2013; van Wilsem 2011; Williams 2016). In the UK study, men, the elderly, and those in higher socio-economic groups were most likely to be victimized, yet these associations were moderated by the introduction of RAT measures, indicating the relevance of target visibility and accessibility in predicting victimization (Reyns 2013). Williams (2016) conducted the largest study of RAT and online identity theft to date, using data from the Eurobarometer Cybersecurity Special Survey. Just over seven per cent of the European population reported being a victim of online identify theft. The routine activities of using ecommerce sites (such as eBay) to sell goods and emailing, and using computers in public settings (e.g., universities and libraries) were predictive of victimization. The guardianship measures installing antivirus, changing passwords and security settings regularly, avoiding using online services and public computers were all statistically associated with victimization. A multilevel analysis of the survey evidenced that the chance of falling victim to online identity theft was not simply reducible to individual routine activities and capable guardianship, and that country of residence explained around 6 percent of the risk of victimization. Based on the statistically significant results reported in these studies of the domestic population, routine activities and capable guardianship measures are tested in the hypotheses below to identify if the same patterns extend to the business population.

Hypotheses

H1: Organization routine activities, such as bring your own devices (BOYD) and remote working, will be associated with increased likelihood of insider cyber victimization.

New technologies in the workplace present opportunities for new routine activities and hence security vulnerabilities for insider victimization. Ponemon (2013) reported that near 50 percent of respondents in a cyber security survey revealed that BOYD had resulted in a significant increase in fraud risk. Similar risks are also presented by the increased use of cloud-based services (such as Dropbox and Google Drive) that can be exploited as part of an attack by client employees or by the external third parties. Social media use is also generating complex new challenges as employees routinely access sites such as Facebook and Twitter in the workplace. Most organizational security models are perimeter based, that is, the control of information requires it to remain within an access-controlled network perimeter. Integrating BYOD, cloud, and social media often leads to de-perimeterization where security technologies become ineffective leading to sensitive organizational information being leaked on such services, either intentionally or unintentionally (Burnap and Hilton 2009). In line with RAT, this hypothesis will test the effect of these routine staff activities on the likelihood of victimization while controlling for organizational characteristics and guardianship practices.

H2: Organization guardianship practices, including presence of security managers, worry of insider threats, and awareness of risks, will be associated with likelihood of insider cyber victimization.

The Cyber Security Breaches Survey 2016 (CSBS 2016) reported that only 28 percent of respondents stated that there was a manager or board member within their organization with responsibility for cyber security. The survey also found that businesses that invest in cyber security are more likely to have experienced breaches than those with lower spending (an unsurprising finding given Williams (2016) shows online criminal incidents often motivate avoidance and security behaviours). In line with RAT, this hypothesis aims to test the association between organization guardianship and insider cyber victimization while controlling for organizational characteristics and routine activities. No direction of association is assumed given previous research that shows precautionary measures taken against crime can be adopted pre- and post-victimization, presenting both positive and negative associations in statistical models based on cross-sectional surveys.

H3: Company characteristics, such as length of incorporation, size, and sector, will be associated with likelihood of insider cyber victimization.

Successive government surveys (ISBS 1998–2015 and most recently the CSBS 2016) have identified that an organization's characteristics impact upon the likelihood of all forms of business cybercrime victimization. For example, the ISBS 2015 reported that insider victimization was up 58 percent for large-sized, and 22 percent forsmall-sized organizations, compared to the previous year. This final hypothesis tests the predictive power of three key organization characteristics as control factors while holding constant routine activities and guardianship factors.

Data and methods

The Cardiff University UK Business Cybercrime Victimization Survey was designed to test RAT within organizational settings. The survey was made up of private sector businesses and was undertaken at enterprise rather than establishment level, so that where a business operates from more than one site, only its head office (not its branches) was contacted. Businesses with no employees, that is, businesses that consist of only a self-employed owner-manager or self-employed

partners, were excluded from the survey. A simple stratified random sample was drawn based on business size and industry sector. The sample specification was based on attaining a minimum number of interviews by business size (number of employees) based on bandings. The employee within the business selected for interview varied. Upon initial contact, it was requested that the interviewer speak to the person in the company with the greatest responsibility of cybersecurity issues. Company directors were typically interviewed in micro and small businesses, while IT and security managers were typically interviewed in medium-sized and large-sized businesses. The interviews were undertaken by BMG Research at its Birmingham-based call center facility, and computer-assisted telephone interviewing (CATI) was used.[4]

Survey data were weighted to reflect the business population distribution as a whole. Because no definitive statistics are available on the level of Internet use by business size and sector, the overall business population, as defined by Inter Departmental Business Register (IDBR) statistics, was used for weighting factors. Consequently, the resulting sample profile reflects that of the overall business population of private sector businesses. Table 1 provides item coding details and descriptive statistics for the variables used in the analysis, including weighted and non-weighted summaries.

Dependent measure

Survey respondents were asked about their organization's experience of insider business cybercrime in the last 3 years. The response options ranged from "none" to "several times a day." A majority of respondents reported experiencing insider cyber victimization no more than "once or twice in the last three years." Therefore, responses were recoded into a binary variable in preparation for logistic regression.

Independent measures

Organization routine activities

Nine organization routine activities were included as potential correlates of insider cyber victimization, derived from the following survey questions, and coded as binary responses: "Which of the following do your company staff use or practice in working hours?: Social media; e-Commerce; Cloud services; Public WiFi; Business WiFi; Mobile devices supplied by organizations; Own devices (BYOD); Remote access" and "Does your company store confidential data?." These are direct measures of routine organization online activities practiced by staff that, if left unguarded, have the potential to expose suitable targets (organization and/or customer) to insiders.[5]

Organization capable guardianship

Guardianship was assessed via a range of direct and indirect measures, in keeping with traditional RAT research (see Wilcox, Madensen, and Tillyer 2008). One binary direct measure of capable guardianship was included based on the survey question: "Is there anyone specifically responsible for managing information security in your company?" Based on evidence that suggests fear and awareness of crime influences perceptions of risk that constrain behavior and redirect from risky routine activities online (Reisig, Pratt, and Holtfreter 2009), two indirect measures of guardianship were included: Worry about insider cyber victimization and Awareness in sector of insider threat risk.

[4]BMG Research is a privately run research consultancy (http://www.bmgresearch.co.uk). They were selected to administer the survey on behalf of Cardiff University following a competitive procurement process. CATI interviewing involves taking survey responses over the telephone and inputting answers into a digital version of the survey. Survey design and data analysis were undertaken by the research team at Cardiff University.

[5]Responses are subject to the respondent or indeed the company IT/security staff knowing what its staff do. Indeed, all cyber security/crime surveys suffer the same problem given lack of knowledge and the "stealth" nature of some forms of cyber (sleeping viruses, etc.).

Organization characteristics

Organization characteristics items from the survey were entered as control covariates in the models. Three covariates were included: Years trading, Organization size, and Sector, all of which are shown in previous research to significantly correlate with cybercrime victimization within organizations (ISBS 2015, CSBS 2016).

Modelling strategy

Dependent and independent variables were entered into three logistic regression models that included the RAT measures. The first model includes only Organization Routine Activities, the second model includes only Organization Guardianship processes, and the final model includes these variables plus Organizational Characteristics. Model fit diagnostics are reported, indicating the amount variance explained in the dependent by the variables in each model.

Findings

Table 1 presents bivariate test results prior to multi-variate modelling. Just under 10 percent of organizations responding to the survey reported experiencing insider cyber victimization. This represents 4.1 percent (48,024) of the population of organizations. Of the organizational characteristics, only size emerged as statistically significant (F = 17.48, p = < .01). Three percent of micro-size organizations (up to 10 employees) reported insider cyber victimization, compared to 7 percent of small-sized (up to 50 employees), 23 percent of medium-sized (up to 250 employees), and 37 percent of large-sized organizations (over 250 employees). This result corroborates the ISBS 2015 finding that showed large organizations were more at risk from this kind of cybercrime, compared to small-sized organizations (75 percent compared to 31 percent). However, the rates of victimization found in our survey are more reliable than those reported in the ISBS 2015, given that our sample is statically representative of organizations in the UK. Several of the bivariate tests for organization routine activities emerged as statistically significant, including use of social media (Adjusted F = 8.54, p = < .01); use of cloud services (Adjusted F = 6.77 p = < .01); use of business WiFi (Adjusted F = 5.85, p = < .05); use of mobile devices (Adjusted F = 19.22, p = < .01); use of remote access (Adjusted F = 37.59, p = < .01); and storing confidential data (Adjusted F = 20.14, p = < .01). Unlike the Ponemon (2013) finding that half of survey respondents reported staff use of their own devices (BOYD) increased fraud, our analysis shows no association (the same applies to the multi-variate findings below). Of the guardianship variables, employing a cyber security manager (Adjusted F = 6.53, p = < .05) and worry about insider victimization (F = 4.79, p = < .05) emerged as significant in the bivariate analyses. All variables were entered into multivariate analysis, the results of which are presented below.

Table 2 presents the results of the three logistic regression models. The Routine Activities Model was significant and explained between 6 and 13 percent of the variance in the likelihood of insider cyber victimization. Of the routine activities reported in the survey, storing confidential data, staff use of mobile devices, and staff use of remote access emerged as statistically significant in predicting victimization, partly supporting hypothesis 1. The other routine activities that emerged as significant in the bivariate analysis—using social media, cloud services and business WiFi—were not predictive when other factors were controlled for. Despite the reported increased risk of these new technologies, their ineffectiveness as insider attack vectors in our models can be explained. Cloud services are likely to have an effective perimeter security model of their own; business WiFi would be encrypted end to end; and social media use may leave users susceptible to other types of cyber victimization but would be unlikely to lead to an attributable insider breach. Holding all other routine activities constant, storing confidential data emerged as most significant (p = < .01). Organizations storing these kinds of data were more likely to experience insider cyber victimisation a factor of 2.85, compared to organizations not storing confidential customer information. This routine organizational activity is associated with insider fraud (e.g., appropriation of confidential information for personal gain) and sabotage (e.g., deletion or modification of data). Staff using mobile devices supplied by organizations emerged as next

Table 1. Descriptive and Bivariate Statistics.

		Sample total		Population total (weighted)		Experienced insider business cybercrime		
Variables	Coding	*N*	%/*M*	*N*	%/*M*	*Yes* (%/*M*)	*No* (%/*M*)	*F test* [a]
Dependent								
Insider business cybercrime	0 = No	680	90.5	1,112,411	95.9			
	1 = Yes	71	9.5	48,024	4.1			
Independent								
Years trading	0 = Less than 10 years	204	27.2	377,062	32.5	5.5	95.5	.130
	1 = 10 years or more	547	72.8	783,373	67.5	3.5	96.5	
Company size	1 = Micro	377	50.2	953,050	82.1	2.8	97.2	***17.482*****
	2 = Small	200	26.6	173,510	15.0	7.2	92.8	
	3 = Medium	125	16.6	27,935	2.4	22.5	77.5	
	4 = Large	49	6.5	5,940	0.5	36.5	63.5	
Industry sector	1 = Manufacturing & Construction	130	17.3	296,975	25.6	4.7	95.3	4.540
	2 = Hospitality & Retail	168	22.4	359,320	31.0	4.3	95.7	
	3 = IT & Finance	217	28.9	129,735	11.2	4.1	95.9	
	4 = Professional Services[b]	236	31.4	374,405	32.3	3.6	96.4	
Staff use social media	0 = No	342	45.5	645,449	55.6	1.9	98.1	***8.535*****
	1 = Yes	409	54.5	514,986	44.4	6.9	93.1	
Staff use e-Commerce	0 = No	493	65.6	845,639	72.9	3.7	96.3	.514
	1 = Yes	258	34.4	314,796	27.1	5.3	94.7	
Staff use cloud	0 = No	403	53.7	783,334	67.5	2.5	97.5	***6.767*****
	1 = Yes	348	46.3	377,101	32.5	7.6	92.4	
Staff use public WiFi	0 = No	604	80.4	940,737	81.1	4.0	96.0	.059
	1 = Yes	147	19.6	219,698	18.9	4.7	95.3	
Staff use business WiFi	0 = No	84	11.2	187,697	16.2	1.5	98.5	***5.845****
	1 = Yes	677	88.8	972,738	83.8	4.7	95.3	
Staff use mobile devices	0 = No	360	47.9	722,950	62.3	1.4	98.6	***19.220*****
	1 = Yes	391	52.1	437,485	37.7	8.6	91.4	
Staff use own devices	0 = No	381	50.7	587,683	50.6	4.3	95.7	0.15
	1 = Yes	370	49.3	572,752	49.4	4.0	96.0	
Staff use remote access	0 = No	303	40.3	648,817	55.9	0.9	99.1	***37.587*****
	1 = Yes	448	59.7	511,617	44.1	8.2	91.8	
Stores confidential data	0 = No	340	45.3	725,722	62.5	1.3	98.7	***20.141*****
	1 = Yes	411	54.7	434,712	37.5	8.9	91.1	
Has a security manager	0 = No	317	42.2	489,135	42.2	1.7	98.3	***6.534****
	1 = Yes	434	57.8	671,300	57.8	5.9	94.1	
Worry insider threat	Scale (1 = not at all to 4 = very)	—	2.10	—	1.86	2.39	1.84	***4.792****
Awareness in sector	Scale (1 = very bad to 5 = very good)	—	3.67	—	3.56	3.54	3.56	.009

Notes: *N* = 751.
[a]Tests performed on weighted sample. For categorical variables Adjusted F score reported using test of independence of rows and columns. For scale variables F score reported based on a two-group one-way analysis of variance.
[b]Includes legal, education and health.
***p = < .05, **p = < .01.**

most significant ($p = < .05$). Organizations providing staff with devices, such as mobile phones and tablets, were more likely to experience insider security breaches by a factor of 2.23, compared to those organizations that did not provide mobile devices to staff. Staff using remote access emerged as least significant ($p = < .05$). Organizations allowing remote access, such as VPN working from home, were more likely to experience victimization, by a factor of 1.96. These effects could be explained by the use of perimeter security models within most organizations. The use of mobile devices and remote access results in the de-perimeterization effect where security controls become ineffective outside of corporate networks (Burnap and Hilton 2009; SANS Institute 2003). The weakening or absence of such controls in tandem with remote access to confidential data can cause a cascade effect, opening up opportunities for all forms of insider victimization.

Table 2. Logistic Regression Estimating Insider Business Cybercrime.

	Routine activities model			Guardianship model			Full model		
	B	S.E.	Exp (B)	B	S.E.	Exp (B)	B	S.E.	Exp (B)
Organization characteristics									
Years trading							−0.51	0.35	0.60
Size									
Micro (ref)									
Small							**0.85***	0.45	2.34
Medium							***1.85****	0.45	6.37
Large							***2.48****	0.52	11.98
Sector									
Professional services (ref)									
Hospitality & retail							−0.30	0.41	0.74
IT & Finance							−0.07	0.39	0.93
Manufacturing & construction							0.38	0.39	1.46
Organization routine activities									
Staff use social media	0.21	0.29	1.23				−0.05	0.31	0.96
Staff use e-Commerce	−0.46	0.28	0.63				−0.42	0.31	0.66
Staff use cloud	0.20	0.29	1.22				0.15	0.31	1.17
Staff use public WiFi	0.28	0.30	1.33				0.09	0.34	1.10
Staff use business WiFi	−0.44	0.42	0.65				−0.45	0.45	0.64
Staff use mobile devices	**0.80***	0.32	2.23				0.39	0.36	1.47
Staff use own devices	−0.02	0.27	0.98				0.19	0.29	1.21
Staff use remote access	**0.67***	0.36	1.96				0.28	0.39	1.32
Stores confidential data	***1.05****	0.34	2.85				**0.90***	0.36	2.47
Organization capable guardianship									
Has a cyber security manager				***0.67****	0.29	1.96	**0.74***	0.32	2.10
Worry insider threat				***0.61****	0.12	1.84	***0.43****	0.13	1.54
Awareness in sector				**−0.27***	0.12	0.76	**−0.32***	0.13	0.73
Constant	−3.71	0.51	0.024	−3.20	0.52	0.04	−4.02	0.82	0.02
Model fit									
Sig.	0.00			0.00			0.00		
Cox & Snell R square	.06			.05			.16		
Nagelkerke R square	.13			.12			.35		
N =	751			751			751		

Notes: * ***p* = < .05, ****p* = < .01.**

The Guardianship Model was also significant and explained between 5 and 12 percent of the variance in the likelihood of insider cyber victimization, roughly equal to the Routine Activities Model. All the guardianship factors reported in the survey, having a dedicated cyber security manager, worry about insider cyber victimization, and awareness of the insider threat risks in the sector, emerged as statistically significant, fully supporting hypothesis 2. Holding all other guardianship factors constant, employing a dedicated cyber security manager emerged as most significant ($p = < .01$). Organizations employing these managers were more likely to have experienced victimization by a factor of 1.96. This replicates the finding in the latest Cyber Security Breaches Survey (2016) and is in line with general victimization studies that show criminal incidents often motivate the adoption of avoidance or security behaviors (Skogan and Maxfield 1981; Williams 2016). It is also plausible that investment in dedicated cyber security staff increases the likelihood of detecting breaches (Williams and Levi 2015). Those with a higher level of worry over insider cyber victimization were also significantly more likely to have experienced a breach ($p = < .01$), compared to those with a lower level of worry. This could mean that they are good at predicting risks, or that as in offline victimization, there may be an increase in worry *post victimization* (McIntyre 1967). Respondents who felt there was a low level of awareness of the risks of insider threats in their sector were also significantly more likely to have experienced victimization ($p = < .05$).

The explanatory power of the Full Model far exceeded that of both sub-models, accounting for between 16 and 35 percent of the variance in the likelihood of insider victimization. However, only one variable was responsible for this increase—size of organization. In line with findings from the 2015 ISBS, neither length of years trading nor sector emerged as significantly predictive of insider victimization, indicating that the

risk of insider attack is evenly distributed over company age and type in the UK (contrary to the US evidence presented by Collins et al. 2016). Several of the routine activities dropped out of significance in the full model—using mobile devices and remote access—indicating that the size of organization is more important for explaining victimization. The size of company alone explains between 9 and 19 percent of the variance in the likelihood of insider cyber victimization (not reported in Table 2), partly supporting hypothesis 3. Compared to micro-size companies (up to 10 employees), large-size companies (over 250 employees) were more likely to suffer victimization by a factor of 11.98, medium-size companies (up to 250 employees) by a factor of 6.37, and small-size companies (up to 50 employees) by a factor of near 2.34.

Discussion

The analysis provides the first evidence that routine activities and guardianship factors within organizations influence the likelihood of insider cyber victimization. Hypothesis 1 was partially supported in the full model, showing the routine activity of storing confidential data increased the likelihood of victimization. However, more guardianship factors emerged as significant in explaining insider threat victimization, fully supporting hypothesis 2. Hiring a security manager was most predictive, followed by worry about breaches and low levels of awareness. With respect to worry, our survey possibly captured both "dysfunctional" worry (concrete emotions) and "functional" worry (motiving precautions) (Grey, Jackson, and Farrall 2010). Extreme worry in the case of insider victimization may therefore be interpreted as motivating the adoption of security measures that assist in anticipating and preparing for threat by promoting vigilance and routine precaution (Borkovec, Alcaine and Behar 2004). This interpretation supports the first guardianship association, where victimization leads to worry, which leads to the hiring of cyber security managers. The relationship between awareness of insider threat risks in the sector and victimization has emerged in the more general Internet security literature (see MacKenzie 1999). Those sectors that engage with new technologies, such as the Internet, to a limited extent might obtain moderate levels of trust in the technology, but the knowledge feeding into this trust may be too shallow to successfully avoid victimization. Indeed, these sectors may take more risks online, given increased confidence but insufficient security knowledge. Those sectors that are closest to the Internet, such as those that exclusively buy and sell online, have a proclivity toward engaging with technical issues, are exposed to more messages about security threats, and are interested and equipped to consume them, resulting in the avoidance of victimization. The final hypothesis was partly supported by the association of organization size and victimization. The effect that medium-sized and large-sized organizations have on the likelihood of victimization is so significant that it deserves unpacking here.

While not featured in this study, there are characteristics of medium-sized and large-sized corporations, other than number of employees, that will impact upon the likelihood of insider cyber victimization. Both in terms of the volume and intensity of potential offenders, and the controls exercised by others in the environments of medium-sized and large-sized organizations, it is important to take account of the roles of procedural legitimacy and corporate culture. Studies of employees show that they are motivated by their evaluations of the legitimacy of corporate rules (Tyler and Blader 2005). Tyler's (Tyler 2006, 2009) analysis of legitimacy and adherence to rules by employees is interesting and empirically grounded; and the flurry of criminal and regulatory cases in 2012–16 covering a range of bank/corporate misconduct occurring over several years in relation to money laundering, diesel emissions, fraud, insider dealing, rogue trading, and terrorist sanctions evasion has reinforced the challenge and importance of corporate culture. Tyler focused on the law-breaking of white-collar *workers* rather than on that of CEOs or other senior employees. Tyler (2009: 199) distinguishes between "compliance with the law and voluntary, willing acceptance of the law," the latter being particularly salient "in work settings," and in our opinion larger organizations, because it predicts rule following even where there is no perceived detection risk. Tyler (2009), Tyler and Blader (2005), and Blader and Tyler (2009) stress the importance of procedural fairness in

generating legitimacy, based on their studies of business rather than government. For the particular case of insider offending *against* their organization, the difficulties start when we look not at the generality of rule-obedience but at exceptions to it. Hollinger and Davis (2005: 214) note that "studies related to equity theories indicate that employee theft is not necessarily an act of greed or opportunity. Instead, employee theft is a consequence of organizational characteristics that produce inequitable relationships. Employees steal to react against, counter, or control injustices in their work environment." They also discuss organizational culture, noting (p.215): "employees appeared to be more constrained by the anticipated reaction from co-workers than by formal reactions from the organizational management. As such, the informal structure is considered the most important factor determining the incident and prevalence of employee theft." In the light of surveys of financial services employees globally, we would expect to see widespread preparedness to subvert organizational goals: given that cyber-related and other risks can occur for organizations anywhere in the world, such findings of dissatisfaction and de-legitimation are important (Nurse et al. 2014). Indeed, there is a lengthy criminological and social psychological literature on "techniques of neutralization" and cognitive dissonance by which we "learn" (often in the workplace setting) to rationalize our behavior as acceptable or innovate to do so, whether from others directly in conversation or—as often in the case of insider cyber cases—in solo contemplation. However, even in a world in which Tyler-like legitimacy efforts are in place to encourage internalised rule-following, some individuals can be deviants who are comfortable in rule-breaking for what they consider to be good reasons. Thus, although the general rate of rule-breaking may be reduced in medium-sized and large-sized organizations that espouse legitimacy, it cannot be guaranteed that it will be reduced to zero.

Conclusion

This study is the first stage in building up the larger picture, by examining how often companies report that insiders do hurt them. The Cardiff University UK Business Cybercrime Survey represents the most robust source of information on insider cybercrime victimization at the time of publication. Just under 1 in 10 companies (9.5 percent) responding to the survey reported experiencing an insider cyber security breach, representing 4.1 percent (48,024) of the population of organizations. This study has explored whether insider cyber security breaches are a function of risky routine activities conducted in organizations employing potential *offenders* (whether motivated or not) who have access to suitable targets in the absence of capable guardianship. All hypotheses were partially supported at each stage of analysis. In the final analysis, the full model indicated that both routine activities (in particular storing confidential data) and guardianship processes were statistically significant in explaining the likelihood of insider cyber victimization. While new technologies in the workplace, such a remote access and mobile devices, present more complex security vulnerabilities, this research shows that organizational characteristics and guardianship practices are more important when predicting insider cyber victimization. This study contributes to the range of crime issues understandable by routine activities theory, showing how it can be applied to insider cyber victimization, and to cybercrime more generally. Future empirical research in this area might focus on the role of perceived legitimacy within organizations in forming part of the motivation for the insider cyber offender.

Funding

This work was supported by the UK Engineering and Physical Sciences Research Council (EPSRC) grant "Identifying and Modelling Victim, Business, Regulatory and Malware Behaviours in a Changing Cyber-Threat Landscape" funded under the Global Uncertainties Consortia for Exploratory Research in Security (CEReS) programm (grant number: EP/K03345X/1).

Notes on contributors

MATTHEW WILLIAMS is Professor of Criminology at Cardiff University, UK. He is Director of the Social Data Science Lab (http://socialdatalab.net/), and lead social science investigator on the UK Engineering and Physical Sciences Research Council (EPSRC) project "Identifying and Modelling Victim, Business, Regulatory and Malware Behaviours in a Changing Cyberthreat Landscape." He is also the UK lead on the National Institute for Justice project "Understanding Online Hate Speech as a Motivator for Hate Crime'. Amongst others he advises the UK Home Office, Metropolitan Police Service (London) and the Welsh Government on cybercrime and cyber-security issues.

MICHAEL LEVI has been Professor of Criminology at Cardiff University, UK since 1991. He has been conducting international research on the control of white-collar and organised crime, corruption and money laundering/financing of terrorism since 1972, and has published widely on these subjects as well as editing major journals. He is currently writing books on White-Collar Crimes and Their Victims and on The Organisation of White-Collar Crimes.

PETE BURNAP is a Reader (Associate Professor) at Cardiff University, UK, and is seconded to Airbus' Digital Transformation Office to lead Cyber Security Analytics Research, heading projects involving the application of Artificial Intelligence, Machine Learning and Statistical Modeling to Cyber Security problems (most recently malware analysis). He has published more than 70 academic articles stemming from funded research projects worth over £10m and has advised the Home Affairs Select Committee, Home Office and Metropolitan Police on socio-technical research outcomes associated with cyber risk and evolving cyber threats.

R.V. GUNDUR is a Lecturer (Assistant Professor) of Criminology at the University of Liverpool in Singapore. He has a doctorate in criminology from Cardiff University. His research focuses on illicit enterprise, gangs, and cybercrime.

References

BIS. 2015. *Information Security Breaches Survey 2015*. London: Department for Business, Innovation and Skills.

Blader, S. L. and T. R. Tyler. 2009. "Testing and Extending the Group Engagement Model: Linkages between Social Identity, Procedural Justice, Economic Outcomes, and Extrarole Behavior." *Journal of Applied Psychology* 94 (2):445–64.

Borkovec, T. D., O. Alcaine, and E. Behar. 2004. ""Avoidance Theory of Worry and Generalized Anxiety Disorder." Pp. 77–108 in *Generalized Anxiety Disorder: Advances in Research and Practice*, edited by, R. G. Heimberg, C. L. Turk, and D. S. Mennin. New York: Guilford Press.

Cohen, Lawrence E. and Marcus Felson. 1979. "Social Change and Crime Rate Trends: A Routine Activity Approach." *American Sociological Review* 44 (4):588–608.

Collins, M., M. Theis, R. Trzeciak, J. Strozer, J. Clark, D. Costa, T. Cassidy, M. Albrethsen, and A. Moore. 2016. *Common Sense Guide to Mitigating Insider Threats*. 5th edn. Software Engineering Institute. Pittsburgh, PA

CSBS. 2016. *Cyber Security Breaches Survey*. London: Department for Culture, Media & Sport.

DCMC. 2016. *Cyber Security Breaches Survey 2016*. London: Department for Culture, Media & Sport.

Gill, Martin. 2005. *Learning from Fraudsters*. London: Protiviti.

Grey, Emily, Jonathan Jackson, and Stephen Farrall. 2010. "Feelings and Functions in the Fear of Crime." *British Journal of Criminology* 51 (1):75–94.

HM Government. 2015. *National Security Strategy and Strategic Defence and Security Review 2015 A Secure and Prosperous United Kingdom*. London: Cabinet Office.

Hollinger, Richard C. and Jason L. Davis. 2005. "Employee Theft and Staff Dishonesty." Pp. 203–28 in *Handbook of Security*, edited by, M. Gill. London: Macmillan.

Holt, Thomas J. and Adam M. Bossler. 2008. "Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization." *Deviant Behavior* 30 (1):1–25.

ISBS. 2015. Information Breaches Survey: Technical Report. London: Department for Business, Energy and Industrial Strategy

SANS Institute. 2003. *Remote Access VPN - Security Concerns and Policy Enforcement*, Available at: https://www.sans.org/reading-room/whitepapers/vpns/remote-access-vpn-security-concerns-policy-enforcement-881. Accessed 6th April, 2018

Levi, Michael, R. V. Alan Doig, David Wall Gundur, and Matthew L Williams. 2016. "Cyberfraud and the Implications for Effective Risk-Based Responses: Themes from UK Research." *Crime, Law and Social Change* 67 (1):77–96.

Levi, Michael and R. V. Gundur. 2015. *Insider Threats: An Exploratory Typology of Published Cases in the Media*, Unpublished Project Report. Cardiff University.

Levi, Michael and Matthew L. Williams. 2013. "Multi-Agency Partnerships in Cybercrime Reduction: Mapping the UK Information Assurance Network Cooperation Space." *Information Management & Computer Security* 21 (5):420–43.

MacKenzie, Donald. 1999. "The Certainty Trough." Pp. 43–46 in *Society on the Line*, edited by, W. H. Dutton. Oxford: Oxford University Press.
Maimon, David, Mariel Alper, Bertrand Sobesto, and Michel Cukier. 2014. "Restrictive Deterrent Effect of a Warning Banner in an Attacked Computer System." *Criminology* 52 (1):33–59.
McIntyre, Jennie. 1967. "Public Attitudes toward Crime and Law Enforcement." *The Annuls of the American Academy of Political and Social Sciences* 374:34–36.
Newman, Graeme R. and Ronald V. Clarke. 2003. *Superhighway Robbery: Preventing E-Commerce Crime*. Portland, OR: Willan Publishing.
Nurse, Jason R., Oliver Buckley, Philip A. Legg, Michael Goldsmith, Sadie Creese, Gordon R. T. Wright, and Monica Whitty. 2014. "Understanding insider threat: A framework for characterising attacks.". Presented at Security and Privacy Workshops, 2014 IEEE. Pp 214–28.
Burnap, Pete and Jeremy Hilton. 2009. "Self Protecting Data for De-Perimeterised Information Sharing." In Proceedings of the 3rd IEEE Int'l Conference on Digital Society, ICDS. Cancun, Mexico.
Ponemon. 2013. *The Risk of Insider Fraud Second Annual Study*. Traverse City, MI: Ponemon Institute.
Pratt, Travis C., Kirsty Holtfreter, and Michael D Reisig. 2010. "Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory." *Journal of Research in Crime and Delinquency* 47 (3):267–96.
Reisig, Michael D., Travis C. Pratt, and Kirsty Holtfreter. 2009. "Perceived Risk of Internet Theft Victimization: Examining the Effects of Social Vulnerability and Financial Impulsivity." *Criminal Justice and Behavior* 36 (4):369–84.
Reyns, Bradford W. 2013. "Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses." *Journal of Research in Crime and Delinquency* 50 (2):216–38.
Skogan, Wesley G. and Michael G Maxfield. 1981. *Coping with Crime: Individual and Neighborhood Reactions*. London: Sage.
Tyler, Tom R. 2006. *Why People Obey the Law*. New Haven: Princeton University Press.
Tyler, Tom R. 2009. "Self-Regulatory Approaches to White-Collar Crime: The Importance of Legitimacy and Procedural Justice." Pp. 195–216 in *The Criminology of White-Collar Crime*, edited by, S. Simpson and D. Weisburd. New York: Springer.
Tyler, Tom R. and Steven L. Blader. 2005. "Can Businesses Effectively Regulate Employee Conduct? the Antecedents of Rule following in Work Settings." *Academy of Management Journal* 48 (6):1143–58.
van Wilsem, Johan. 2011. "Worlds Tied Together? Online and Non-Domestic Routine Activities and Their Impact on Digital and Traditional Threat Victimization." *European Journal of Criminology* 8 (2):115–27.
Wall, David S. and Matthew L. Williams. 2007. "Policing Diversity in the Digital Age: Maintaining Order in Virtual Communities." *Criminology and Criminal Justice* 7 (4):391–415.
Wall, David S. and Matthew L. Williams. 2013. "Policing Cybercrime: Networked and Social Media Technologies and the Challenges for Policing." *Policing and Society* 23 (4):409–12.
Wilcox, Pamela, Tamara D. Madensen, and Marie S. Tillyer. 2008. "Guardianship in Context: Implications for Burglary Victimization Risk and Prevention." *Criminology* 45 (4):771–803.
Williams, Matthew L. 2006. *Virtually Criminal: Crime, Deviance and Regulation Online*. London: Routledge.
Williams, Matthew L. 2007. "Policing and Cybersociety: The Maturation of Regulation within an Online Community." *Policing and Society* 17 (1):59–82.
Williams, Matthew L. 2016. "Guardians upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level." *British Journal of Criminology* 56 (1):21–48.
Williams, Matthew L and Michael Levi. 2015. "Perceptions of the eCrime Controllers: Modelling the Influence of Cooperation and Data Source Factors." *Security Journal* 28 (3):252–71.